Healthcare Security Lessons From the Field

Increase security and take the pain out of HIPAA compliance

securityMETRICS®

About this ebook

Who should read this ebook?

- Officers, practitioners, and managers of HIPAA compliance and data security at small, medium, and large covered entities
- Managers of HIPAA compliance and data security for business associates
- Anyone involved in network, data, or patient information security

What does this ebook include?

- Five lessons learned from commonly overlooked security errors made by healthcare entities and business associates
- Reasons why these errors are important to fix
- How to remediate these security errors to make your organization more secure and take the pain out of the HIPAA compliance process

Who is SecurityMetrics?

SecurityMetrics has helped over one million organizations comply with HIPAA, PCI DSS, and other mandates. Our solutions combine innovative technology that streamlines validation with the personal support you need to fully understand compliance requirements. You focus on the business stuff—we've got compliance covered.

Learn more about us at
www.securitymetrics.com

Introduction

With over 10 years of security assessment and audit experience, we have seen wide ranges of network environment complexity, IT staff experience, and executive team support. **One consistency in the overwhelming majority of our assessments are deficiencies in data security,** even in well-established organizations employing experienced IT staff.

This ebook covers five lessons we've learned from the most commonly overlooked security errors we see in healthcare organizations. Learning about, identifying, and resolving these security mishaps in your organization will not only increase your security, but also help you take the pain out of the HIPAA compliance process.

Today's lessons:

1. Understand your data flow
2. Keep systems updated
3. Treat policies and procedures as more than paperwork
4. Employ secure access controls
5. Be thorough in your risk analysis

Understand your data flow

In order to protect your patient data you must understand the flow of protected health information (PHI) throughout your network. Your PHI flow includes where PHI enters, moves, and is stored in your system.

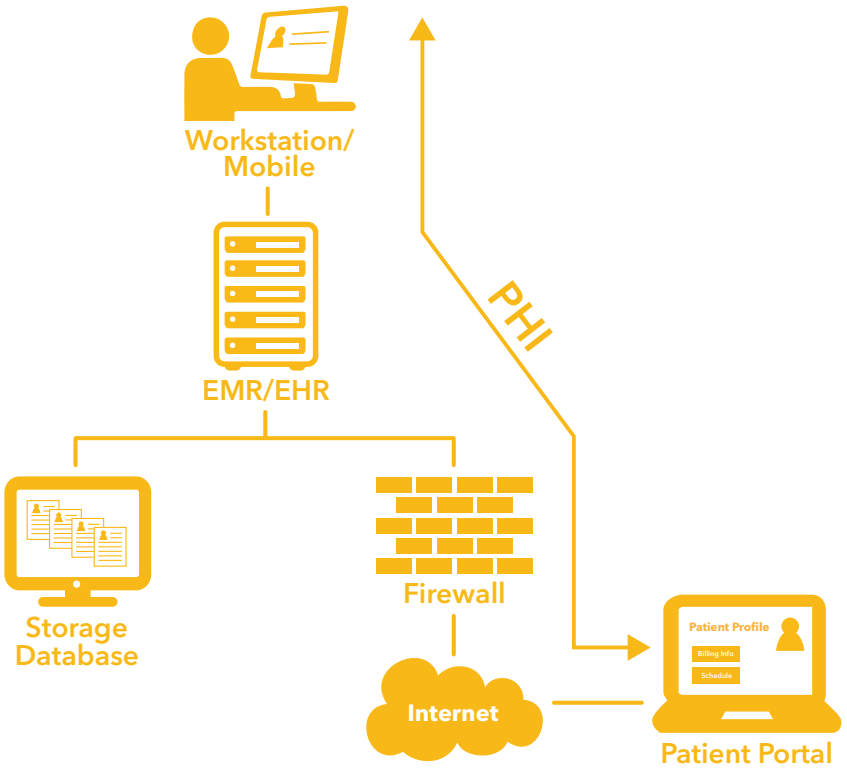
From the field

A lack of communication between departments can lead to not understanding your data flow, which often creates security and compliance issues.

During an onsite interview with customer service representatives, we discovered they were recording PHI in notebooks or Excel spreadsheets for future reference. These new copies of PHI were not protected or encrypted in any way. In fact, one representative showed us her desk drawer with dozens of notebooks filled with PHI. Not only is unencrypted PHI a HIPAA violation and security issue, but the fact that the organization was unaware of this practice is a big problem.

Take the pain out of HIPAA compliance

Fully understanding where PHI resides takes a lot of interdepartmental communication. Consult with all departments and individuals that collect, enter, store, transmit, or interact with PHI and create a PHI flow diagram based on your findings. (see example below). This exercise will assist in conducting a thorough risk analysis and identify where to focus security measures at your organization to adequately protect PHI.



Keep systems updated

Attackers look for low hanging fruit. If there is a known security flaw in a system, they will target organizations in hopes they have not installed updates containing essential security patches.

From the field

Often, organizations will not install updates out of convenience. Sometimes they fear it will break current processes. We conducted an assessment of an organization whose main server hadn't been patched for 12 years! Needless to say, the system had a vast number of vulnerabilities. The owner hadn't applied patches because he was convinced patching the system would break his processes. Eventually, he had to replace the entire system because getting to current patch levels would be too difficult.

Take the pain out of HIPAA compliance

Your HIPAA Security Officer (if you don't have one, designate one today!) should make sure all available software updates have been completed, including Internet browsers, firewalls, electronic health record (EHR) systems, point-of-sale (POS) terminals, MS Office, etc.

Moving forward, updates should be implemented as soon as they are available and documented when completed. Installing software updates that contain essential security enhancements is required by HIPAA and is one of the most effective ways to avoid vulnerability exploitation.

Recent HIPAA breach

Central Utah Clinic, 2014
31,000+ patient records

This breach could have been prevented by patching vulnerabilities with vendor-supplied security updates and running periodic vulnerability scans.

Treat policies and procedures as more than paperwork

HIPAA requirements on policies and procedures may take up an entire shelf or filing cabinet at your office, if not more. Not only are policies and procedures a foundational part of many HIPAA requirements, they also play a crucial role in real life compliance and security.

From the field

We have worked with entities unfortunate enough to have undergone an OCR audit or investigation. During interviews, OCR auditors review policies and procedures, interview staff, and observe the actual procedure in action. If all three of these factors don't match exactly hefty fines may be issued (see chart below).

Violation Category	Penalty	Maximum per Calendar Year
(A) Did not know	$100-$50,000	$1,500,000
(B) Reasonable Cause	$1,000-$50,000	$1,500,000
(C) (i) Willful Neglect-Corrected	$10,000-$50,000	$1,500,000
(C) (ii)Willful Neglect-Not Corrected	$50,000	$1,500,000

We recently interviewed Doreen Espinoza, Business Development and Privacy Officer of Utah Health Information Network (UHIN), who underwent an OCR pilot audit in 2012. She provided the OCR 127 documents as part of her audit.

Take the pain out of HIPAA compliance

Conduct a formal review of your policies and related procedures annually to ensure they are up to date and match what is happening in 'real life'. Conduct trainings to implement these policies and help employees understand the 'why' behind policies and procedures. Providing the 'why' helps build a culture of security in your organization, leading to a more complete policy implementation.

Employ secure access controls

A business' first line of defense between it and the Internet is through access controls, also known as firewall rules. Most threats can be blocked by simply and selectively restricting access to places in the PHI environment. This not only includes preventing unauthorized inbound attempts into the PHI environment, but also unauthorized outbound access from inside the PHI environment by trusted employees.

From the field

Unfortunately, secure access controls are rarely set up correctly. In fact, we see insecure inbound and outbound firewall rules in 90% of first time assessments. It's common for people to make outbound access rules overly permissive, or protect the wrong systems from malicious inbound traffic.

One IT staff we worked with had a new system they needed to add to their environment immediately. In the rush, they couldn't get the access controls right, so they added a firewall rule allowing all traffic in and out. The problem was, this quick fix made all other rules in the firewall irrelevant. The IT staff fully intended to fix it later, but forgot about it and the firewall was left in an open state. If a hacker had found their network, they could have easily been compromised.

Take the pain out of HIPAA compliance

Don't make security choices based on convenience. Review your access controls and determine if you need to make adjustments based on security. Don't forget the outbound rules! If correctly configured, these rules will increase your security, help prevent attackers from getting to PHI, and ensure your compliance with HIPAA requirements.

Don't make security choices based on convenience.

Be thorough in your risk analysis

As part of the Security Rule The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) requires covered entities and business associates to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of protected health information (PHI) held by the organization".

Conducting a thorough risk analysis includes analyzing how data is collected, listing all systems that interact with PHI, identifying potential threats and vulnerabilities, assessing current security measures, and documenting all findings.

From the field

Many organizations have checked off the risk analysis box. The problem is, many of these risk analyses are not thorough and complete.

One of our clients had already 'completed' a risk analysis with another vendor just a few months prior to our risk analysis. However, we found many vulnerabilities not mentioned or reviewed in the initial risk analysis. Among others, these vulnerabilities included no database encryption, no internal or external network scans, and a shared firewall password. These are very serious vulnerabilities, which had slipped through their less than thorough risk analysis.

Take the pain out of HIPAA compliance

Research risk analysis best practices, including HHS' guidance, and involve a security expert when conducting a risk analysis. Use the results of your risk analysis to help create a risk management plan, which will include controls or mitigation strategies for each identified risk.

Prioritize your risk management plan to implement controls that will mitigate the highest risks first, based on NIST SP 800-30 Impact Definitions (see table below). Resolving the highest risks first will make the greatest positive security impact while getting you closer to achieving full HIPAA compliance.

Risk	Impact Definition (NIST SP 800-30)
High	Exercise of the vulnerability (1) may result in the highly costly loss of major assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

Conclusion

Without thorough preparation, most covered entities and business associates would fail a HIPAA audit. Without a background in security there are many security aspects covered entities and business associates might never consider. If you implement the five lessons in the ebook, you'll be way ahead of most, and much more resistant to compromise.

For more information about how we can help you protect your patient data and simplify HIPAA compliance contact us at 801.705.5656 or HIPAA@securitymetrics.com.

How vulnerable is your patient data?

HIPAA requires you to run periodic vulnerability scans. **Learn** how to locate external network vulnerabilities before criminals do.